Mozes Magyar
mmagyar
20247055

1.
    (a) The current name of the NSA program is Bullrun. The codename of the GCHQ program is Edgehill.
    (b) Britain, Canada, Australia, New Zealand and the US have access to the program; the name of the group is “Five Eyes”.
    (c) SSL, https, SSH, encrypted chat, VPNs, and encrypted VOIP are technologies that are targeted by the program.
    (d) The NSA is able to recover plaintext messages, as said “The encryption documents now show, in striking detail, how the agency works to ensure that it is actually able to read the information it collects. ” in the http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption article
    (e) Google, Yahoo, Facebook and Microsoft’s Hotmail are the “big four” companies targeted by GCHQ.
    (f) “the consumer” is one of the adversaries according to the leaked documents, while “terrorists, cybercriminals, human traffickers and others ” are the adversaries according to the articles.
2.
    (a) An example of each of hardware, software, and data with respect to network routers is the physical router itself, Cisco IOS, and the traffic entering and leaving the router, respectively.
    (b) An example of interception would be forwarding sensitive data to a third party as well as its intended recipient. An example of interruption would be disabling all traffic on a port. An example of modification would be changing the routing table to give priority to an analyzing computer and that update would propagate to neighbouring routers, this is also an interception attack but it modifies the way the local area acts instead of just the one router. An example of fabrication would be capturing packets to resend them later to redo a transaction.
    (c)
        i. The article speculates the method of attack is “pre-written scripts or backdoor tools and root kits for attacking known but unpatched vulnerabilities in these systems, as well as for attacking zero-day vulnerabilities that are yet unknown to the vendor and customers. ”.
        ii. Yes, there is a greater opportunity to attack a router.
        iii. The motive for attacking a router instead of a specific user is “because it [gives] agencies access to data from entire networks of computers instead of just individual machines”.
3.
    (a) Tip 1 is an example of deterrence because making yourself harder to find is one of the definitions given from the notes. Tip 2 is an example of deterrence because encrypted traffic is harder to use than plaintext traffic. Tip 3 is an example of deflection because just any Joe Schmo is probably not up there on the 'to spy on' list, which should be good enough for most users. Tip 4 is an example of prevention because is you stick to smaller companies or open-source encryption, it's more likely to avoid letting in backdoors. Tip 5 is an example of prevention for the same reasons as tip 4.

Mozes Magyar
mmagyar
20247055

(b) The technique that best describes the defence outlined in the article is detection because knowing that a service isn't compromised and then them now saying they are no longer not compromised is exactly what detection is.

(c) The NIST is a standards organization that has likely been influenced by the NSA, as shown on http://it.slashdot.org/story/13/09/11/1224252/are-the-nist-standard-elliptic-curves-back-doored. AES is an elliptic-curve standard that has likely been weakened by the NSA, as shown by Silent Circle's move away from AES, as shown on http://www.pcworld.com/article/2051380/silent-circle-moves-away-from-nist-cryptographic-standards-cites-uncertainty.html.

Exploits

1. The vulnerability done in sploit1 is in check_forbidden it uses arg[1] as the format string. It does a combination of Direct Parameter Access with Short Write to write the address of the given shellcode into the retloc of the check_forbidden function. It writes X characters then looks at parameter 105, which contains the address of check_forbidden's retloc and writes X there, which are bytes in the address of the shellcode, which is given as arg[2]. It then does the same for Y characters, etc, to write the rest of the address of the shellcode into check_forbidden's retloc to execute the shellcode.
   A way to repair this would be to change line 365 from printf(source); to printf("%s",source); which doesn't appear to suffer from the same vulnerability.
2. The vulnerability done in sploit2 is in print_version, it is almost the same as sploit1, using a format string vulnerability, but with different addresses and parameter offsets.
   A way to repair this vulnerability would be to change line 37 from printf(txt); to printf("%s", txt);
3. The vulnerability exploited in sploit3 is a buffer overflow in copy_file. The way I exploited is taken nearly verbatim from the overflow reading except instead of passing it to submit as an argument it is written to a file and the file is read into the submit program where it overflows the buffer for transferring files. It works because the link(...) function on line 82 fails because it would appear that the share directory is on a different partition.
   A way to repair this vulnerability would to read a character then write a character, never keeping a buffer or to read at most sizeof(buf)-1 characters then writing that many characters to file.
4. I don't know what to call the vulnerability exploited in sploit4, but it exploits the relative path of mkdir being supplied on line 158 instead of an absolute path. The program creates a valid C program then compiles it to an executable named mkdir and changes the path environment variable to include at the front of it the /share directory. It works because the very first time submit runs, it creates the directory for the user to submit to. When it does try to make the directory the first time, instead the program created by sploit4 is run, which changes the path variable to what SU what see and runs a shell.